County of Inyo
Request for Information (RFI)
RFI-IS-2003

Network Firewalls
September 2020

Submit Proposals via email to:

sarmstrong@inyocounty.us

Date Released:

September 23, 2020

Submittal Deadline:

October 16, 4:30 p.m.

Table of Contents

I.   Introduction

Brief

The County of Inyo is requesting information about available firewalls or other network security devices. The information will be used to aid the County in redesigning our network security infrastructure in order to improve security, performance, and reliability.

Requested Information

The following information is being requested:

- Available firewall models that satisfy the requirements listed in the **Scope** section (page 4).
- Approximate per-unit pricing (for relative comparison between models only).
- Approximate recurring or subscription costs.
- Other ideas or recommendations based on the information provided in the **Scope** section.

Audience

Any company or individual is welcome to respond to this RFI with the requested information.

Notices

This RFI is issued as a means of technical discovery and information gathering only.

This RFI is for planning purposes and is not a competitive solicitation, nor does it imply any obligation on the County's part to enter into any contract or to make any purchase.

The County may use the results of this RFI in drafting a competitive solicitation (RFP) at a later date.

Participation in this RFI is voluntary and those submitting responses do so entirely at their expense. There is no expressed or implied responsibility on the part of the County to reimburse respondents for any expenses incurred in preparing or submitting their responses.

II.   Scope

The classifications below are based on the network diagram on page 6.

The specifications listed are <u>minimum</u> requirements, with notes indicating options we would like to see if they're available, but that aren't necessarily required.

Classifications

All Firewalls
- Exception logging and reporting
- [option]: Centralized management
- [option]: Centralized logging and reporting

Remote FW
- Firewall for remote site – standard firewall with site-to-site (split tunnel) VPN to the main County network.
- Typically supports fewer than 20 clients.
  - Site-to-site (split-tunnel) VPN

VPN FW
- VPN concentrator for all remote site-to-site tunnels.
- Potentially also supporting mobile, user-based VPNs.
  - 1 Gbps ports
  - Support up to 25 site-to-site VPNs
  - [option]: Mobile, user-based VPNs

Internet FW
- Internet firewall for outbound traffic and inbound tunnels.
- Primary outbound route for some clients and failover route for others.
- Re-routes to a different Internet gateway in the event of an outage.
- Typically supports up to 250 clients, or up to 600 during failover scenarios.
  - Advanced inbound filtering (country or risk-based)
  - Tagged VLANs
  - Internet gateway failover routing
  - [option]: TOR exit node filtering
  - [option]: Attack/scan/anomaly detection and prevention

HA FW
- High-availability firewalls. Same as **Internet FW**, but able to operate as an HA pair.
- Typically supports up to 350 clients, or up to 600 during failover scenarios.
  - High-availability configuration (active/active or active/passive)
  - Advanced inbound filtering (country or risk-based)
  - Tagged VLANs
  - Internet gateway failover routing
  - [option]: TOR exit node filtering
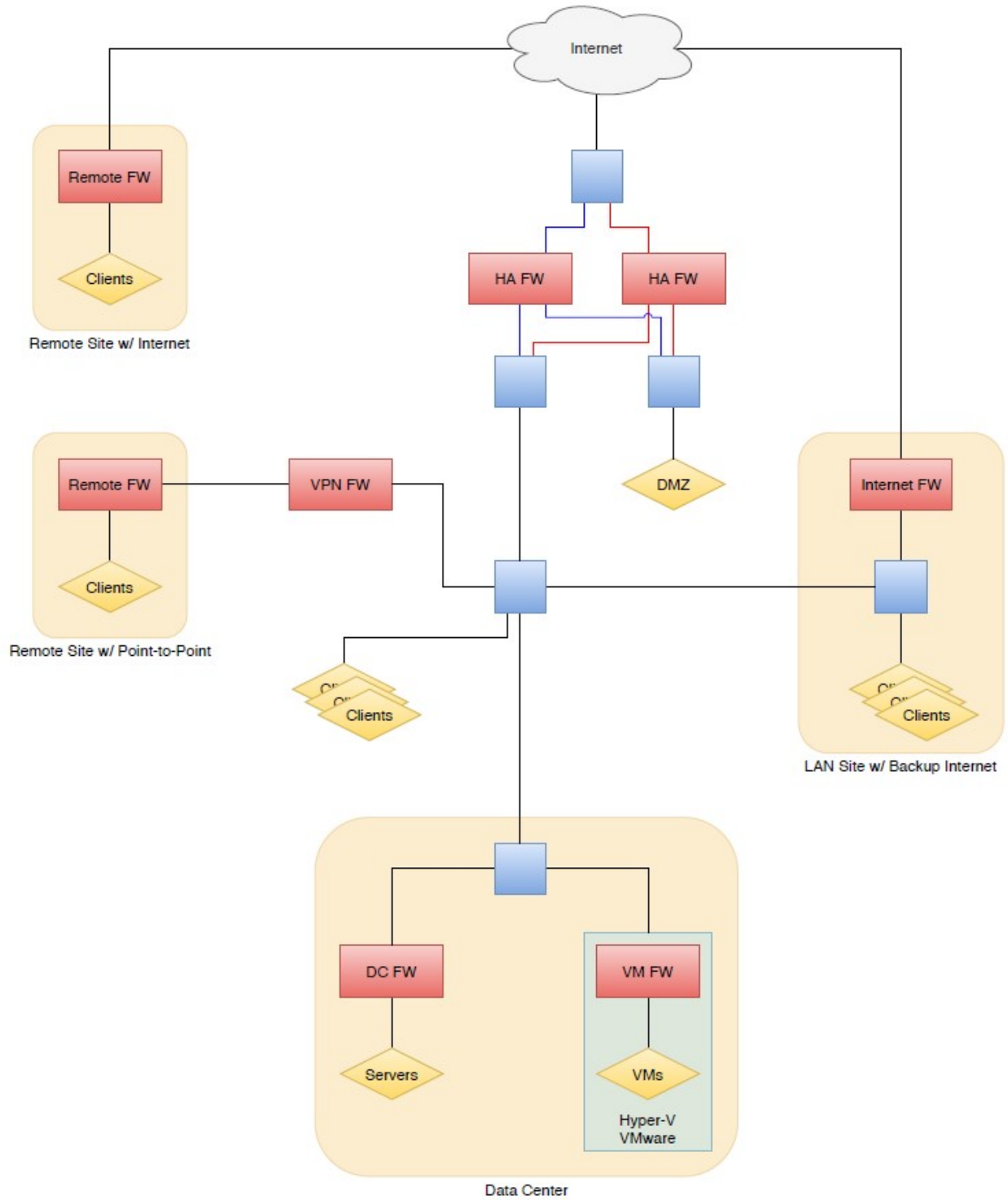 - [option]: Attack/scan/anomaly detection and prevention

DC FW

- High-throughput data center firewall to control traffic to, from, and between servers in the data center.
    - Tagged VLANs
    - 1 Gbps and 10 Gbps ports

VM FW

- Virtual firewall to control traffic to, from, and between virtual machines running on the same host server.
    - Hyper-V support
    - VMware support

III.   Network Diagram

IV.   Responses

Deadline

The deadline for submitting information for the Network Firewalls RFI is October 16, 4:30 p.m.

Response Format

Use the following format in developing a response to our request for information.
Feel free to include additional information that you feel is relevant.

- Clearly identify on the cover that your response is for the Network Firewalls RFI (RFI-IS-2003) for the County of Inyo, California.
- For each of the firewall classifications listed in the **Scope** section, provide a list of models that best meet the requirements for that classification. If more than three models meet the requirements, indicate the top three models that you feel would be the most appropriate for the given application.
- Provide detailed specification and feature information for each of the different models listed in the previous step. Optionally, include "ballpark" or MSRP pricing information.
- Indicate any relevant features that require recurring or subscription costs.
- [Optional] Provide a description of what makes your devices or software stand out above other vendors or manufacturers.
- [Optional] Provide up to three technical examples (e.g. network diagrams) of existing deployments using your equipment, that are similar in nature to what's presented in the **Scope** section (page 4).
- [Optional] Provide any additional ideas or recommendations you have for us, given the information in the **Scope** section.

Submission Information

Responses should be delivered as PDF files via E-mail to Scott Armstrong, sarmstrong@inyocounty.us

Inquiries and County Contact

> Scott Armstrong, Information Services Director
> County of Inyo
> P.O. Box 477
> Independence, CA. 93526
> Email: sarmstrong@inyocounty.us

All inquiries should be directed via email to Scott Armstrong, Director of Information Services, County of Inyo. The closing time for inquiries related to this RFI is October 14th, 4:30 p.m. All inquiries and the associated County responses will be posted on the County website. Interested parties are cautioned that the opportunity to obtain additional information should not be viewed as a sales presentation opportunity.